UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY
TRENTON DIVISION

JESSICA SCHROEDER, individually and on behalf of all others similarly situated, Plaintiff, v. HEALTHEC, LLC, Defendant.	CASE NO.: JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jessica Schroeder ("Plaintiff"), by and through the undersigned counsel, brings this class action complaint against Defendant HealthEC, LLC ("HealthEC" or "Defendant"), on behalf of herself and all others similarly situated. Plaintiff makes the following allegations based upon personal knowledge as to her own actions and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. On December 22, 2023, HealthEC, a New Jersey-based population health management platform that services 26 clients across 18 states—most of which are major healthcare service providers and state-level health systems—disclosed that it was the subject of a massive data breach whereby hackers gained unauthorized access to its networks between July 14 and July 23, 2023 (the "Data Breach"). Upon information and belief, the Data Breach impacted nearly 4.5 million individuals who received care through HealthEC's clients, such as Beaumont ACO, State

of Tennessee – Division of TennCare, and the University Medical Center of Princeton Physicians' Organization, among 14 others.

2. The hackers were able to access, copy, and exfiltrate highly-sensitive information stored on HealthEC's servers, including "name, address, date of birth, Social Security number, Taxpayer Identification number, Medical Record number, Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location), Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (including but not limited to patient account number, patient identification number, and treatment cost information)" ("Protected Health Information" or "PHI").[1]

3. The Data Breach occurred because HealthEC failed to implement reasonable security procedures and practices, failed to disclose material facts surrounding its deficient data security protocols, and failed to timely notify the victims of the Data Breach.

4. As a result of HealthEC's failure to protect the sensitive information it was entrusted to safeguard, Plaintiff and class members now face a significant risk of medical-related identity theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

PARTIES

5. Plaintiff Jessica Schroeder is a resident of Roseville, Michigan whose PHI was exfiltrated from HealthEC.

[1] *See Notice of the HealthEC LLC Cyber Security Event*, HEALTHEC, LLC, https://www.healthec.com/cyber-incident/ (last visited Jan. 4, 2024).

6. Defendant HealthEC, LLC is a population health management platform that is registered in Delaware with its principal place of business in Edison, New Jersey.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from HealthEC. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

8. This Court has jurisdiction over HealthEC because it maintains and operates its headquarters in this District. Defendant HealthEC is authorized to and conducts business in this District and is subject to general personal jurisdiction in this state.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events and omissions giving rise to this action occurred in this District, including unknown actors accessing and copying PHI of patients associated with University Medical Center of Princeton Physicians' Organization located in Somerset County, New Jersey.

FACTUAL ALLEGATIONS

HealthEC's Privacy Practices

10. HealthEC is a population health management company that uses artificial intelligence to "ingest[] all available data – integrating clinical with claims data to create a community health record for each patient."[2] As part of this integration process, HealthEC shares

[2] *Homepage*, HEALTHEC.COM, https://www.healthec.com/ (last visited Jan. 4, 2024).

information between healthcare providers by "connecting everyone across any healthcare system…" [3]

11. HealthEC is affiliated with more than 1 million healthcare professionals and over 8 million members through servicing 26 clients in 18 states.[4]

12. HealthEC contracts with healthcare systems and providers "to identify high-risk patients, close care gaps and recognize barriers to optimal care." [5] To this end, HealthEC obtains third-party patients' personal information, including their full names, home addresses, dates of birth, email addresses, social security numbers, and medical information such as medical histories, past treatment records, prescription information, health provider information, and health insurance coverage, from the health systems that HealthEC services. It then stores this highly-sensitive information on centralized servers maintained by HealthEC.

13. As a result, healthcare patients do not voluntarily provide their PHI to HealthEC, but rather, HealthEC obtained their information from the health systems that it services.

14. Given the amount and sensitive nature of the data it collects, HealthEC maintains a "Privacy Policy" which describes how confidential patient information is used and disclosed. HealthEC represents that it: "is committed to protecting the privacy of the personally-identifiable information that we collect from you…"[6] HealthEC boasts that it "has implemented generally accepted standards of technology and operational security in order to protect Personal Info from

[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Privacy Policy*, HEALTHEC.COM, https://mneconnect.healthec.com/ProdMNeConnectAdmin/Privacy_Policy.aspx (last visited Jan. 4, 2024).

loss, misuse, alteration, or destruction. Only authorized HealthEC personnel are provided access to Personal Info, and these employees are required to treat this information as confidential."[7]

15. Given its avowed experience in its field handling highly sensitive PHI, HealthEC understood the need to protect patients' PHI and prioritize data security.

The Data Breach

16. Between July 14 and July 23, 2023, hackers infiltrated HealthEC's networks and accessed highly sensitive patient information stored on its servers. HealthEC disclosed that once it discovered the intrusion, it "promptly began an investigation" and also "notified federal law enforcement regarding the event and cooperated with their investigation."

17. According to HealthEC, the investigation revealed "that certain systems were accessed by an unknown actor between July 14, 2023, and July 23, 2023, and during this time certain files were copied."

18. The investigation confirmed that extensive personal medical information was accessed and copied, including patient's full names, dates of birth, Social Security numbers, Taxpayer Identification numbers, Medical Record numbers, Medical information (including but not limited to Diagnosis, Diagnosis Code, Mental/Physical Condition, Prescription information, and provider's name and location), Health insurance information (including but not limited to beneficiary number, subscriber number, Medicaid/Medicare identification), and/or Billing and Claims information (including but not limited to patient account number, patient identification number, and treatment cost information).

[7] *Id.*

19. HealthEC acknowledged this information was not only accessed but also copied from its servers. A disclosure by HealthEC to the Department of Health and Human Services revealed that the breach impacted 4,452,782 individuals.

20. HealthEC did not disclose the existence of the Data Breach to the affected third-party patients until December 22, 2023, when it began mailing individual notification letters—five months after the initial breach.

The Data Breach was Preventable

21. Following the Data Breach, HealthEC stated that it "take[s] this event, your privacy, and the security of information in [its] care very seriously" and among other things, it is "reviewing [its] existing policies and procedures."

22. Upon information and belief, these "existing policies and procedures" were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred. This is especially true given that the healthcare industry is frequently one of the most targeted sectors for cyberattacks and attacks using stolen credentials have increased precipitously over the last several years.

23. Healthcare providers and their affiliates like HealthEC are prime targets because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and personal information of employees and patients—all extremely valuable on underground markets.

24. This was known and obvious to HealthEC as it observed frequent public announcements of data breaches affecting healthcare providers and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of hackers.

25. The Department of Health and Human Services (HHS) recently disclosed that in 2023 alone more than 88 million individuals have been subjected to healthcare-related data breaches, a staggering 60% increase from the prior year.[8]

26. It is well known that use of stolen credentials through long been the most popular and effective method of gaining authorized access to a company's internal networks and that companies should activate defenses to prevent such attacks.

27. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[9] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[10]

28. The risk is so prevalent for healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory" warning that they have "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[11] The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI issued the advisory to warn healthcare providers to take "timely and reasonable precautions to protect their networks from these threats."[12]

---

[8] HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation, https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html (last visited Jan. 4, 2024).

[9] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Jan. 4, 2024).

[10] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Jan. 4, 2024).

[11] https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Jan. 4, 2024).

[12] *Id.*

29. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or others users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains only one different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or to download an attachment containing malware.

30. User education provides the easiest method to assist in properly identifying fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from CISA, organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[13]

31. From a technical perspective, companies can also greatly reduce the flow of fraudulent e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security measures governing e-mail transmissions, including Sender Policy Framework (SPF) (e-mail authentication method used to prevent spammers from sending messages on behalf of a company's domain), DomainKeys Identified Mail (DKIM) (e-mail authentication method used to ensure messages are not altered in transit between

[13] https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 4, 2024).

the sending and recipient servers), and Domain-based Message Authentication, Reporting and Conformance (DMARC), which "builds on the widely deployed [SPF] and [DKIM] protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email."[14]

32. Additionally, because the goal of these schemes is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access, even if an individual's login credentials are disclosed. For example, multi-factor authentication is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

33. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies

[14] *Id.*

can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

34. Network segmentation is commonly used in conjunction with the principle of least privilege (POLP), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[15] In an example given by security software provider Digital Guardian:

> [A]n employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide.[16]

This is precisely why approximately 67% of targeted malware and stolen credential schemes are directed at individual contributors and lower-level management personnel.[17]

35. In addition to mitigating the risk of stolen credentials, the CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to latest available versions, prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;

[15] https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited Jan. 4, 2024).
[16] *Id.*
[17] https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited Jan. 4, 2024).

- Employing best practices for use of Remote Desktop Protocol (RDP) as threat actors often gain initial access to a network through exposed and poorly secured remote services; and

- Disabling operating system network file sharing protocol known as Server Message Block (SMB) which is used by threat actors to travel through a network to spread malware or access sensitive data.[18]

36. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[19]

37. Despite holding the PHI of millions of patients, HealthEC failed to adhere these recommended best practices. Indeed, had HealthEC implemented common sense security measures like network segmentation and POLP, the hackers never could have accessed millions of patient files and the breach would have been prevented or much smaller in scope. HealthEC also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

38. HealthEC, like any entity in the healthcare industry its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. HealthEC's belated review of its procedures and policies is inexcusable given its knowledge that it was a prime target for cyberattacks.

[18] CISA Guide at 4.
[19] *Id.* at 5.

Allegations Relating to Plaintiff Jessica Schroeder

39. Plaintiff Jessica Schroeder lives and resides in Roseville, Michigan and is a former healthcare patient of one of HealthEC's clients.

40. For purposes of receiving medical treatment, Ms. Schroeder was required to provide her healthcare provider with her sensitive personal information, including, among other information, her full name, home address, date of birth, e-mail address, Social Security number, health insurance ID card, and driver's license.

41. Ms. Schroeder's healthcare provider also maintained her patient account numbers, health insurance plan member ID numbers, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

42. Ms. Schroeder's healthcare provider shared Ms. Schroeder's PHI with HealthEC in connection with her treatment.

43. In December 2023, Ms. Schroeder received a notification letter from HealthEC stating that she was a victim of the Data Breach. The letter stated that: "[w]e are writing to make you aware of a data incident that may impact the privacy of some of your information we received in connection to your relationship with Beaumont ACO."

44. The letter recommended that Ms. Schroeder take certain actions like monitoring her financial accounts, explanation of benefits statements, and monitoring credit reports for suspicious activity and to detect errors. Furthermore, the letter recommended that Ms. Schroeder place a "fraud alert" or "security freeze," if not both, on her credit report to detect any possible misuse of personal information.

45. As a result of the Data Breach, Ms. Schroeder has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of

unauthorized activity, which she will continue to do indefinitely. Ms. Schroeder also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical-related identity theft or fraud, and any number of additional harms against her for the rest of her life.

HealthEC Failed to Comply with Federal Law and Regulatory Guidance

46. HealthEC is a healthcare provider covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

47. These rules establish national standards for the protection of patient information, including PHI, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

48. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[20]

49. HIPAA requires that HealthEC implement appropriate safeguards for this information.[21]

[20] 45 C.F.R. § 164.502.
[21] 45 C.F.R. § 164.530(c)(1).

50. HIPAA requires that HealthEC provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.* non-encrypted data.[22]

51. Despite these requirements, HealthEC failed to comply with its duties under HIPAA and its own Privacy Policy. Indeed, HealthEC failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the PHI of its patients and employees;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

[22] 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

52. Additionally, federal agencies have issued recommendations and guidelines to help minimize the risks of a data breach for businesses holding sensitive data. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices, which should be factored into all business-related decision making.[23]

53. The FTC's publication *Protecting Personal Information: A Guide for Business* sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[24] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[25]

54. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security; monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[26] This is consistent with guidance provided by the FBI, HHS, and the principles set forth in the CISA 2020 guidance.

---

[23] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 4, 2024).

[24] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 4, 2024).

[25] *Id*.

[26] FTC, *Start With Security*, *supra* note 41.

55. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[27]

56. HealthEC was fully aware of its obligation to implement and use reasonable measures to protect the PHI of the third-party patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. HealthEC's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

The Impact of the Data Breach on Victims

57. The PHI exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit medical-related identity theft and fraud, one of the most dangerous and costly forms of identity theft.

58. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or

[27] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 4, 2024).

drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[28]

59. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an individual."[29] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[30]

60. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[31]

[28] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited Jan. 4, 2024).
[29] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Jan. 4, 2024).
[30] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 4, 2024).
[31] https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Jan. 4, 2024).

61. Indeed, while federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[32] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[33]

62. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[34]

63. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[35]

64. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the

[32] https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 ("Ponemon Study") (last visited Jan. 4, 2024).
[33] *Id*. at 9.
[34] *Id*. at 2.
[35] *Id*. at 14.

resolution of the crime.[36] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[37]

65. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[38]

66. Perhaps most dangerous, however, is the potential for misdiagnoses or treatment. According to Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care

[36] *Id*. at 1.
[37] *Id*.
[38] https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Jan. 4, 2024).

was delayed because there was confusion about what was true in their records due to the identity theft."[39] This echoes the Ponemon study, which notes that "many respondents are at risk for further theft or errors in healthcare records that could jeopardize medical treatments and diagnosis."[40]

67. According to a Consumer Reports article entitled *The Rise of Medical Identity Theft*, this outcome "isn't a hypothetical problem" as the "long tail on medical identity theft can create havoc in victims' lives."[41] As one example, a pregnant woman reportedly used a victim's medical identity to pay for maternity care at a nearby hospital. When the infant was born with drugs in her system, the state threatened to take the *victim's* four children away—not realizing her identity had been stolen. The victim ultimately had to submit to a DNA test to remove her name from the infant's birth certificate, but it took years to get her medical records corrected.[42]

68. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[43] According to Tom Kellermann, "Traditional criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[44] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

---

[39] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Jan. 4, 2024).
[40] Ponemon Study at 1.
[41] https://www.consumerreports.org/medical-identity-theft/medical-identity-theft/ (last visited Jan. 4, 2024).
[42] *Id.*
[43] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Jan. 4, 2024).
[44] *Id.*

69. Given the confirmed copying of PHI from HealthEC's systems, many victims of the Data Breach have likely already experienced significant harms as the result of the Data Breach, including, but not limited to, medical-related identity theft and fraud. Plaintiff and class members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for unauthorized activity.

70. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; and
- 7% reported feeling suicidal.[45]

71. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms

[45] https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last Jan. 4, 2024).

- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[46]

72. The unauthorized disclosure of the sensitive PHI to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[47]

73. Consumers are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense.

74. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiff and class members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the value of the explicit and implicit promises of data security;

c. identity theft and fraud resulting from the theft of their PHI;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. anxiety, emotional distress, and loss of privacy;

---

[46] *Id.*

[47] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial and investment account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued, imminent, and certainly impending injury flowing from potential fraud and identify theft posed by their PHI being in the possession of one or many unauthorized third parties.

75. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

76. There may also be a significant time lag between when personal information is stolen and when it is misused for fraudulent purposes. According to the Government Accountability Office, which conducted a study regarding data breaches: "law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[48]

[48] http://www.gao.gov/new.items/d07737.pdf (last visited Jan. 4, 2024).

77. Plaintiff and class members place significant value in data security. According to a survey conducted by cyber-security company FireEye Mandiant, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[49]

78. Because of the value consumers place on data privacy and security, healthcare providers with robust data security practices are viewed more favorably by patients and can command higher prices than those who do not. Consequently, had third-party patients known the truth about HealthEC's data security practices—that it did not adequately protect and store their PHI —they would not have sought medical care from health systems contracted with HealthEC or would have paid significantly less. As such, Plaintiff and class members did not receive the benefit of their bargain with HealthEC because they paid for the value of services they did not receive.

79. Plaintiff and class members have a direct interest in HealthEC's promises and duties to protect their PHI, *i.e.*, that HealthEC *not increase* their risk of identity theft and fraud. Because HealthEC failed to live up to its promises and duties in this respect, Plaintiff and class members seek the present value of identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by HealthEC's wrongful conduct. Through this remedy, Plaintiff and class members seek to restore themselves and class members as close to the same position as they would have occupied but for HealthEC's wrongful conduct, namely its failure to adequately protect Plaintiff's and class members' PHI.

[49] https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Jan. 4, 2024).

80. Plaintiff and class members further seek to recover the value of the unauthorized access to their PHI permitted through HealthEC's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PHI is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiff and class members have a protectible property interest in their PHI; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

81. HealthEC's deficient notice letter also caused Plaintiff and class members harm. For example, the objective of almost every data breach is to gain access to an organization's sensitive data so that the data can be misused for financial gain. Furthermore, the letter did not explain the precise nature of the attack, the identity of the hackers, or the number of individuals affected. HealthEC's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By waiting months to disclose the Data Breach, HealthEC prevented victims from

taking meaningful, proactive, and targeted mitigation measures that could help protect them from harm.

82. Because HealthEC continues to hold the PHI of third-party patients, Plaintiff and class members have an interest in ensuring that their PHI is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

84. Plaintiff seeks relief in her individual capacity and as a representative of all others who are similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff brings this action on behalf of herself and the Class defined as: All individuals whose personal information was compromised in the Data Breach announced by HealthEC in or about December 2023 (the "Class").

85. Specifically excluded from the Class are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Class are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

86. Class Identity: The members of the Class are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact class members.

87. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. HealthEC's disclosures reveal that the Class contains nearly 4.5 million individuals whose PHI was compromised in the Data Breach.

88. Typicality: Plaintiff's claims are typical of the claims of the members of the Class because all class members had their PHI compromised in the Data Breach and were harmed as a result.

89. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has no known interest antagonistic to those of the Class and her interests are aligned with Class members' interests. Plaintiff was subject to the same Data Breach as class members, suffered similar harms, and faces similar threats due to the Data Breach. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including data breach cases involving multiple classes and data breach claims.

90. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiff and class members a duty to implement and maintain reasonable security procedures and practices to protect their PHI;

b. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

c. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and class members' PHI;

d. Whether Defendant violated its duty to implement reasonable security systems to protect Plaintiff's and class members' PHI;

e. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and class members;

f. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

g. Whether Plaintiff and class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of medical information;

h. Whether Defendant provided timely notice of the Data Breach to Plaintiff and class members; and

i. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

91. Defendant has engaged in a common course of conduct and Plaintiff and class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect patients' PHI, as well as Defendant's failure to timely alert affected customers to the Data Breach.

92. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would

create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under the applicable rules.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

94. Defendant required Plaintiff and class members PHI as a condition of receiving healthcare services and to perform Defendant's AI-driven analytics in connection with providing medical treatment. Defendant collected and stored the data for purposes of providing medical treatment as well as for commercial gain.

95. Defendant owed Plaintiff and class members a duty to exercise reasonable care in protecting their PHI from unauthorized disclosure or access. Defendant acknowledged this duty in its Privacy Policy, where it promised not to disclose PHI without authorization.

96. Defendant owed a duty of care to Plaintiff and class members to provide adequate data security, consistent with industry standards, to ensure that Defendant's systems and networks adequately protected the PHI.

97. As a healthcare provider, Defendant had a special relationship with Plaintiff and class members who entrusted Defendant to adequately safeguard their confidential personal, financial, and medical information.

98. Defendant's duty to use reasonable care in protecting PHI arises as a result of the parties' relationship, as well as common law and federal law, including the HIPAA regulations described above and Defendant's own policies and promises regarding privacy and data security.

99. Defendant knew, or should have known, of the risks inherent in collecting and storing PHI in a centralized location, Defendant's vulnerability to network attacks, and the importance of adequate security.

100. Defendant breached its duty to Plaintiff and class members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PHI of Plaintiff and class members;

b. Failing to comply with industry standard data security measures for the healthcare industry leading up to the Data Breach;

c. Failing to comply with its own privacy policies;

d. Failing to comply with regulations protecting the PHI at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of Defendant's network and systems;

f. Failing to recognize in a timely manner that PHI had been compromised; and

g. Failing to timely and adequately disclose the Data Breach.

101. Plaintiff's and class members' PHI would not have been compromised but for Defendant's wrongful and negligent breach of its duties.

102. Defendant's failure to take proper security measures to protect the sensitive PHI of Plaintiff and class members as described in this Complaint, created conditions conducive to a

foreseeable, intentional criminal act, namely the unauthorized access and copying of PHI by unauthorized third parties. Given that healthcare providers are prime targets for hackers, Plaintiff and class members are part of a foreseeable, discernible group that was at high risk of having their PHI misused or disclosed if not adequately protected by Defendant.

103. It was also foreseeable that Defendant's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiff and class members.

104. As a direct and proximate result of Defendant's conduct, Plaintiff and class members have and will suffer damages including: (i) the loss of rental or use value of their PHI; (ii) the unconsented disclosure of their PHI to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PHI; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PHI for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

105. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

106. As a healthcare provider, Defendant is covered by HIPAA, 45 C.F.R. § 160.102, and is therefore obligated to comply with all rules and regulations under 45 C.F.R. Parts 160 and 164.

107. 45 C.F.R. Part 164 governs "Security and Privacy," with Subpart A providing "General Provisions," Subpart B regulating "Security Standards for the Protection of Electronic Protected Health Information," Subpart C providing requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governing "Privacy of Individually Identifiable Health Information."

108. 45 C.F.R. § 164.104 states that the "standards, requirements, and implementation specifications adopted under this part" apply to covered entities and their business associates, such as Defendant.

109. Defendant is obligated under HIPAA to, among other things, "ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information." 45 C.F.R. § 164.306.

110. 45 C.F.R. Sections 164.308 (Administrative safeguards), 164.310 (Physical safeguards), 164.312 (Technical safeguards), 164.314 (Organizational requirements), and 164.316 (Policies and procedures and documentation requirements) provide mandatory standards that all covered entities must adhere to.

111. Defendant violated HIPAA by failing to adhere to and meet the required standards as set forth in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

112. Likewise, HIPAA regulations require covered entities "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach" to "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of" a data breach. 45 C.F.R. § 164.404. The notice must also contain a minimum amount of information regarding the breach (including the dates of the breach and its discovery), the types of protected health information that were involved, steps individuals should take to protect themselves from harm resulting from the breach, a description of what the entity is doing to investigate the breach and mitigate harm, and contact information to obtain further information. *Id*.

113. Defendant breached its notification obligations under HIPAA by failing to give timely and complete notice of the breach to Plaintiff and class members.

114. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

115. HIPAA further requires Defendant to disclose the unauthorized access and theft of the PHI to Plaintiff and class members "without unreasonable delay" so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and detect misuse of their PHI. See 45 C.F.R. § 164.404.

116. Defendant violated HIPAA by failing to reasonably protect Plaintiff's and class members' PHI and by failing to give timely and complete notice, as described herein.

117. Defendant's violations of HIPAA constitute negligence *per se*.

118. Plaintiff and class members are within the class of persons that HIPAA and its implementing regulations were intended to protect.

119. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

120. Additionally, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PHI. 15 U.S.C. § 45(a)(1).

121. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

122. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI and failing to comply with applicable industry standards. Defendant's conduct was unreasonable given the nature and amount of PHI they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiff and class members.

123. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

124. Plaintiff and class members are within the class of persons that the FTC Act was intended to protect.

125. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and class members. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and class members sustained

actual losses and damages as alleged herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT III
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

126. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

127. Acting in the ordinary course of business, HealthEC entered into contracts with health systems to provide AI-enabled, population health management services using patients' PHI received from the health system.

128. Upon information and belief, each of those respective contracts contained provisions requiring HealthEC to protect the patient information that HealthEC received in order to provide such population health management services in carrying out the business.

129. Upon information and belief, these provisions requiring HealthEC acting in the ordinary course of business to protect the personal information of the third-party patient's was intentionally included for the direct benefit of Plaintiff and class members, such that Plaintiff and class members are intended third party beneficiaries of these contracts, and therefore entitled to enforce them.

130. Defendant breached these contracts while acting in the ordinary course of business by not protecting Plaintiff's and class member's personal information, as stated herein.

131. As a direct and proximate result of Defendant's breaches, Plaintiff and class members sustained actual losses and damages described in detail herein. Plaintiff and class members alternatively seek an award of nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

132. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

133. Plaintiff and class members have an interest, both equitable and legal, in their PHI that was conferred upon, collected by, and maintained by the Defendant and which was stolen in the Data Breach. This information has independent value.

134. Plaintiff and class members conferred a monetary benefit on Defendant in the form of payments for medical and healthcare services, including those paid indirectly by Plaintiff and class members to Defendant.

135. Defendant appreciated and had knowledge of the benefits conferred upon it by Plaintiff and class members.

136. The price for medical and healthcare services that Plaintiff and class members paid (directly or indirectly) to Defendant should have been used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

137. Likewise, in exchange for receiving Plaintiff's and class members' valuable PHI, which Defendant was able to use for their own business purposes and which provided actual value to Defendant, Defendant was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures.

138. As a result of Defendant's conduct, Plaintiff and class members suffered actual damages as described herein. Under principals of equity and good conscience, Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds they received from Plaintiff and class members, including damages equaling the difference in value between medical and healthcare services that included

implementation of reasonable data privacy and security practices that Plaintiff and class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

139. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

140. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

141. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and class members from further cyberattacks and data breaches that could compromise their PHI.

142. Defendant still possesses PHI pertaining to Plaintiff and class members, which means their PHI remains at risk of further breaches because Defendant's data security measures remain inadequate. Plaintiff and class members continue to suffer injuries as a result of the compromise of their PHI and remain at an imminent risk that additional compromises of their PHI will occur in the future.

143. Pursuant to the Declaratory Judgment Act, Plaintiff seeks a declaration that: (a) Defendant's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) Defendant must have

policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry-standard security measures, including, but not limited to, those listed at (ii), (a)-(i), *infra*, and must comply with those policies and procedures; (2) Defendant must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiff's and class members' PHI if it is no longer necessary to perform essential business functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Encrypting PHI and segmenting PHI by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of its systems;

e. Purging, deleting, and destroying in a reasonable and secure manner PHI not necessary to perform essential business functions;

f. Conducting regular database scanning and security checks;

g. Conducting regular employee education regarding best security practices;

h. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as class representatives and Plaintiff's counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of their unlawful acts, omissions, and practices;

F. That Plaintiff be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial in the instant action.

Dated: January 5, 2024

By: /s/ *James E. Cecchi*

James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
jcecchi@carellabyrne.com

Norman E. Siegel*
J. Austin Moore*
Stefon J. David*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
david@stuevesiegel.com
**Pro Hac Vice Forthcoming*

Counsel for Plaintiff and the Class